LAW OFFICE OF
ZACHARY MARGULIS-OHNUMA

October 13, 2015

Via ECF and U.S. Mail

Hon. Sterling Johnson, Jr.
United States District Court
Eastern District of New York
225 Cadman Plaza East
Brooklyn, NY 11201

RE: U.S. v. Adamou Djibo, 15 Cr. 88 (SJ)

Dear Judge Johnson:

This office represents the defendant Adamou Djibo in the above-captioned case. I write in response to the government's letter dated October 5, 2015 and in further support of the defendant's motion to suppress the fruits of a warrantless search and interrogation of him at John F. Kennedy Airport on February 3, 2015.

As the Court has noted and I wish to make here explicit, it is the defendant's position that the forensic search of Mr. Djibo's cellular phone at the airport – which the government seeks to minimize as a "preliminary peek into the phone at the border" – was unlawful. Therefore, any fruits of that illegal forensic search, including all the material obtained pursuant to the search warrant, are subject to suppression.[1]

[1] Mr. Djibo previously argued that the fruits of the search warrant are subject to suppression because the successful execution of the search warrant relied on the involuntary statement Mr. Djibo made at the

260 MADISON AVENUE • NEW YORK, NY 10016
(212) 685-0999 • ZACH@ZMOLAW.COM
WWW.ZMOLAW.COM

1. THE WARRANTLESS SEARCHES AT THE AIRPORT VIOLATED THE FOURTH AMENDMENT

The government maintains in its October 5 letter that the detention, border search, arrest, interrogation, strip search, and forensic electronics search of Mr. Djibo as he was trying to board a plane at John F. Kennedy Airport were all "routine" and therefore lawful; it nonetheless concedes that it "does not intend to use the records obtained from the border search at trial." Gov't 10/5/15 Letter at 2. The government does, however, intend to rely on the fruits of that search, i.e. the cell phone seized from Mr. Djibo and the data found on that cell phone after a search warrant was issued for it. As discussed below, because the warrantless search was unlawful, the cell phone and its contents should be suppressed.

The agents' warrantless search of Mr. Djibo went well beyond the boundaries of a routine border search. After Mr. Djibo was placed in custody, the officers' conduct was more akin to a search incident to arrest. Mr. Djibo was singled out by agents for an outbound search that had nothing to do with customs controls. He was forced out of the boarding line and required to turn over his travel documents, his electronic devices, and the passwords for his devices. He was arrested and strip searched. See 7/13/15 Suppression Hearing Transcript at 24. Most importantly, after he was arrested, agents removed his phone, and, apparently, other devices, and attached them to a Cellebrite forensic machine for analysis that could not be done by simply perusing the phone by hand. The forensic analysis was only done after Mr. Djibo was placed under arrest and "after the border search was complete." Id.

In his testimony Special Agent Thomas Wilbert was evasive about the warrantless forensic search of the devices, revealing its existence only after the Court sua sponte

---

airport in which he was required by agents to state his iPhone passcode. See Djibo 7/1/15 Letter at 5-7. We respectfully submit that both points independently provide sufficient grounds to suppress all information obtained from the phone.

brought him back for a second round of questioning. Although Agent Wilbert testified that another agent "wr[o]te a report based on those searches," i.e. the warrantless forensic searches of Mr. Djibo's devices after his arrest, the government was unable to produce a written report by an agent. 7/29/15 Suppression Hearing Transcript at 71. Instead, the government turned over a series of 71 HTML files that appear to have been generated from the search that night.[2] It is impossible to determine whether these files are a complete report of the search that was done.[3] The agent who actually did the search, identified by Agent Wilbert as Agent Pauta, was not called as a government witness and did not testify.

The government argues that the seizure of the phone and use of the Cellebrite machine was "lawfully conducted pursuant to CBP and HSI's border search authority," and cites cases suggesting that warrantless routine, non-invasive searches at international borders are permitted. 10/5/15 Gov't Letter at 1. But none of these cases involves a forensic analysis of a personal electronic device, which is far more invasive than a manual review of a cell phone during a border search. Moreover, the government's cases pre-date Riley v. California, 134 S. Ct. 2473, 2485 (2014), which held that police "must generally secure a warrant before conducting" a search of a cell phone incident to an arrest. In this case, according to Agent Wilbert, the forensic search of the cell phone took place a "half hour to an hour after the arrest." 7/29/15 Tr. at 71. By that time, any conceivable justification for a warrantless border search was gone: the phone was seized and being held as evidence; there was no way it was going to enter or leave the country other than under law enforcement control. Accordingly, there was no exigency or other rationale that

[2] These are the files contained on the disk that the government provided to the court with its October 5, 2015 letter. The government and Agent Wilbert collectively refer to them as the "report."

[3] Although we had previously requested all forensic reports from the phone under Rule 16 and it was clearly discoverable, the government only disclosed it after Agent Wilbert was required by the Court to acknowledge its existence.

could justify a warrantless search. See Riley v. California, 134 S. Ct. at 2494 (exigent circumstances exception may apply to cell phone searches, but no mention of border exception). The search itself was highly invasive. It produced at least 71 separate files that make up the "report" referred to in Agent Wilbert's testimony. One of these files contains more than 1300 text messages, many of them both intimate and revealing. The agent who actually conducted the search did not testify and the report was not provided until after the agent involved in the arrest and initial, unlawful search had testified.[4]

Finally, the government takes pains to distinguish this case from U.S. v. Kim, No. 13-0100 (ABJ), 2015 WL 2148070, in which the district court for the District of Columbia recently suppressed evidence derived from a warrantless border search of a laptop computer. The government argues that the agents here had more grounds for suspicion than the agents in Kim and that the search was less intrusive. But these are differences of degree, not of kind. In this case, the government set out to arrest Mr. Djibo and searched his cell phones with a forensic device incident to that arrest, after the arrest was effected and after it was clear that Mr. Djibo would not be leaving the country that night. In Kim, the defendant was not arrested at the time of the search but was permitted to board his flight after his electronic devices were seized. Accordingly, the Riley rule did not apply in Kim, but it clearly applies here: absent particularized exigent circumstances, searches incident to arrest require a warrant. Riley v. California, 134 S. Ct. at 2485.

2. THE APPROPRIATE REMEDY IS SUPPRESSION OF THE PHONE AND ITS CONTENTS AS FRUITS OF THE UNLAWFUL SEARCH

The government presented evidence purporting to show that even if agents obtained Mr. Djibo's passcode unlawfully,

[4] In the event that the Court does not agree that the search was invasive and therefore non-routine, we respectfully request an opportunity to examine the agent who conducted the search, Agent Pauta, about the extent of the search and the contents of the report.

they did not need it to access the phone in the subsequent searches. Though the government cites no legal authority, this argument appears to be an invocation of the "inevitable discovery" rule, but fails because it lacks a factual basis. See Nix v. Williams, 467 U.S. 431 (1984) (seminal Supreme Court case on inevitable discovery). In the Second Circuit, "illegally-obtained evidence will be admissible under the inevitable discovery exception to the exclusionary rule only where a court can find, with a high level of confidence, that each of the contingencies necessary to the legal discovery of the contested evidence would be resolved in the government's favor." U.S. v. Heath, 455 F.3d 52, 60 (2d Cir. 2006); accord U.S. v Stokes, 733 F.3d 438, 446 (2d Cir. 2013). "[P]roof of inevitable discovery 'involves no speculative elements but focuses on demonstrated historical facts capable of ready verification….'" U.S. v. Eng, 971 F.2d 854, 859 (2d Cir. 1992).

As we noted previously, the contents of the phone could not have been accessed without the passcode, which was involuntarily provided by Mr. Djibo when he was stopped at the border. The government's argument that it could have used IP Box, a Chinese "hacker tool," to break into the phone is little more than speculation by an agent investigating the case. As was made clear at the hearings, the hacker tool at issue has never been shown to be capable of breaking into the operating system present on the target phone, iOS 8.1.2. The agent declined to test it on a phone running iOS 8.1.2 or higher and relied on nothing more than rumors from individuals he was unable to identify for his conclusion that IP Box could have worked on Mr. Djibo's phone without destroying the evidence on it. Accordingly, the government has not shown "with a high level of confidence" that it could have accessed Mr. Djibo's phone without forcing him to provide his passcode. The inevitable discovery doctrine does not apply.

3. INFORMATION OBTAINED VIA THE SUBSEQUENT SEARCH WARRANT SHOULD BE SUPPRESSED BECAUSE THE GOVERNMENT HAS NOT SHOWN AN INDEPENDENT SOURCE FOR THE INFORMATION CONTAINED IN THE WARRANT APPLICATION

Finally, having grudgingly revealed the existence of the unlawful forensic search, the government now argues – again without citation to legal authority – that the fruits of the search warrant are admissible even if the initial forensic search was unlawful because the warrant application relied on information independent of the illegal search. This appears to be an invocation of the "independent source" doctrine recognized by the Supreme Court in Murray v. U.S., 487 U.S. 533 (1988). The Second Circuit has explained that when the government relies on an independent source, it must show that (1) the warrant is "supported by probable cause derived from sources independent of the illegal entry; and (2) the decision to seek the warrant [was] not [] prompted by information gleaned from the illegal conduct." U.S. v. Johnson, 994 F.2d 980 (2d Cir. 1993).

We respectfully submit that the government has not made a sufficient showing that the independent source doctrine should apply in these circumstances. Nothing was stopping the agents from obtaining a warrant prior to their "preliminary peak" with the Cellebrite machine except that they found it inconvenient to do so. Contrary to the government's assertions, the name of the co-conspirator was found on the iPhone in the "preliminary peak."[5] If they had not found the co-conspirator's name in this initial forensic analysis, a further forensic analysis may not have seemed worthwhile. Moreover, in order to identify the phone in the search warrant, they needed the IMEI number, which is a unique identifier that was been obtained from the initial forensic search. Based on the numbering of the files and lack of testimony from Agent Pauta, it is unclear

[5] This can be confirmed by referring to the disk that the government sent to the Court on Cotober 5, 2015, which contains a file name "/Report_SMSSection(51) with many texts.html". Line 1089 of this file refers to the alleged co-conspirator.

whether the full scope of the "preliminary peak" has been revealed by the government. Accordingly, the government has not shown that the probable cause set forth in the search warrant was truly independent or that the agents would have sought a search warrant at all if they had not unlawfully searched the phone incident to Mr. Djibo's arrest at the airport. As the Sixth Circuit has noted, "'[p]olice who believe they have probable cause to search cannot enter a home without a warrant merely because they plan subsequently to get one.'" U.S. v. Buchanan, 904 F.2d 349, 357 (6th Cir. 1990), quoting U.S. v. Griffin, 502 F.2d 959 (6th Cir. 1974).

Conclusion

Because Mr. Djibo's iPhone was illegally searched in violation of the Fourth Amendment, and because he was unlawfully required to provide his passcode, all information derived from the iPhone should be suppressed.

Thank you for your attention to this case.

Very truly yours,

Zachary Margulis-Ohnuma

Zachary Margulis-Ohnuma

CC: Karen Koniuszy, Esq. (via ECF)